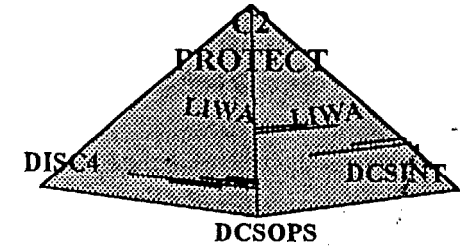# INFORMATION WARFARE

Protecting Friendly Command and Control Capability

The Army's C2 Protect Efforts an In Process Review

LTC MIKE BROWN

HQDA, , DISC4

SAIS-C4C, 703-697-1474

MR PHILLIP LORANGER

HQDA, DISC4

SAIS-C4C, 704-696-8070

C2 Protect - "Keeping The Highway Secure & Open For Force XXI"

Form SF298 Citation Data

Report Date ("DD MON YYYY") 01051995	Report Type N/A	Dates Covered (from... to) ("DD MON YYYY")

Title and Subtitle Protecting Friendly Command and Control Capability The Armys C2 Protect Efforts an In Process Review		Contract or Grant Number
		Program Element Number
Authors		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) HQDA		Performing Organization Number(s)
Sponsoring/Monitoring Agency Name(s) and Address(es)		Monitoring Agency Acronym
		Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms		
Document Classification unclassified		Classification of SF298 unclassified
Classification of Abstract unclassified		Limitation of Abstract unlimited
Number of Pages 34		

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	5/1/95	Briefing

4. TITLE AND SUBTITLE
Information Warfare - Protecting Friendly Command and Control Capability: The Army's C2 Protect Efforts an In Process Review

5. FUNDING NUMBERS

6. AUTHOR(S)
Mike Brown | Phillip Loranger

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis
Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE

A

13. ABSTRACT *(Maximum 200 Words)*
This briefing is a roadmap for the U.S. Army as they move to Command and Control (C2) Protect in support of the Army's Force 21transition. It addresses C2 protect in a digital battlefield environment, the threat and vulnerabilities environment, and Approach to the problem of C2 Protect.

14. SUBJECT TERMS
IA

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

FORCE

Force XXI is:

✓ Integrating and leveraging Information Technology

✓ Redesigning the Tactical Forces

✓ Re-engineering of the base

- Dominate Maneuver
- Win the Info War
- Precision Strike
- Project & Sustain
- Protect the Force

Information is: Power

"...Operate in an unpredictable and changing environment, throughout the depth (and altitude) of the Battle Space (all the way back to the CONUS and/or forward base);

Simultaneously execute, mount, and recover from operations ranging from war to PKO; orchestrate all the operating systems; and do all of this very, very quickly.

The quantum competitive advantage — will derive from the quantity, quality and usability of the information.

The architecture of Force XXI must derive from a robust, versatile concept of information based Battle Command."

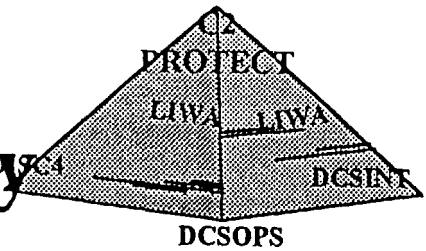GEN Gordon R. Sullivan
March 1994

FORCE XXI

Force XXI
# The Army of the 21st Century

DCSOPS

We will Create Learning
Organizations

- Organized around information — not hardware
- Inherently versatile at every level
- Simultaneously execute, plan, recover-continuous operations
- Leverage skip echelon and split based operations
- Shared situational awareness, not the same map sheet, the same map
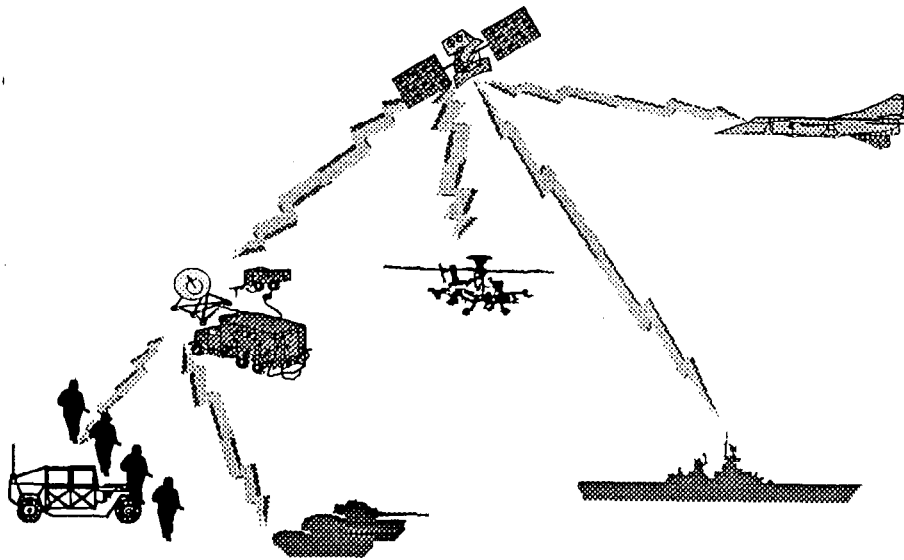
Redesign the Force

. . . Front ⬦ Rear

C2 Protect - "Keeping The Highway Secure & Open For Force XXI"

Information Warfare
An Army Perspective
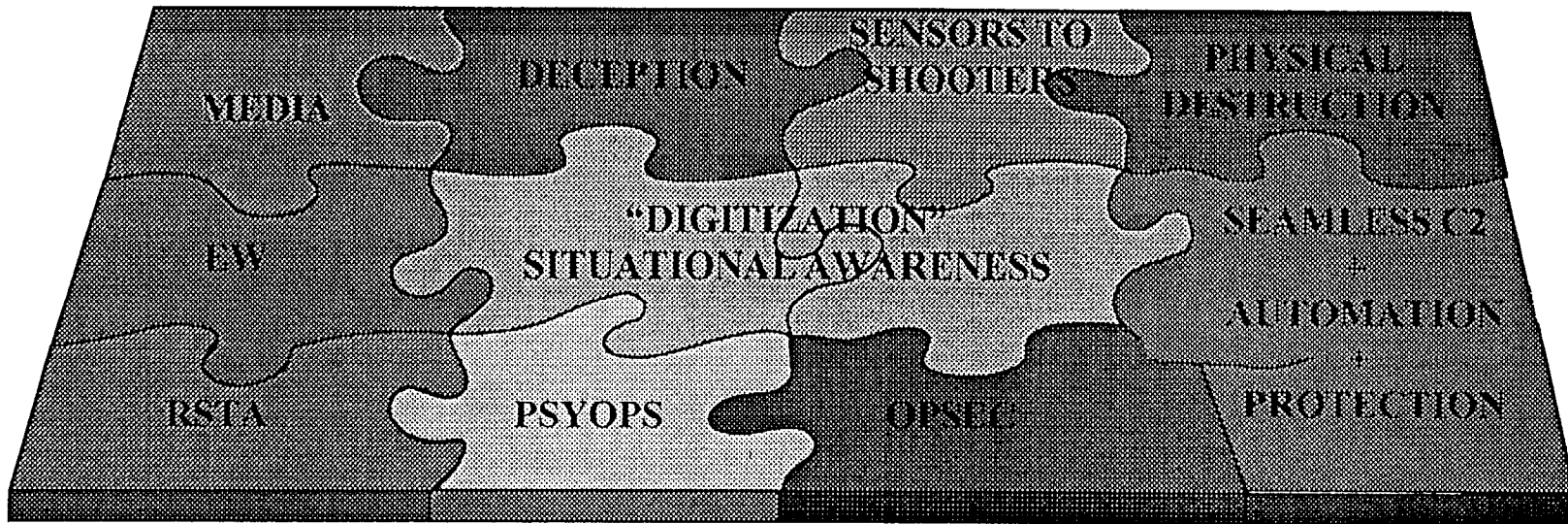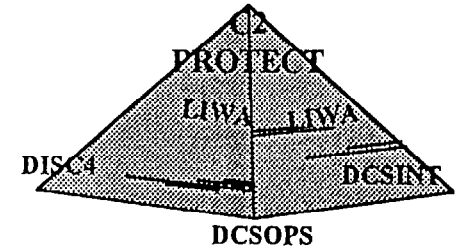
FM 100-6 (Draft)
"INFORMATION OPERATIONS"
Continuous COMBINED ARMS OPERATIONS that enable and protect the
commander's decision cycle while influencing an opponent's Accomplished through
command and control and intelligence operations, Information Operations are
conducted across the full range of military operations.

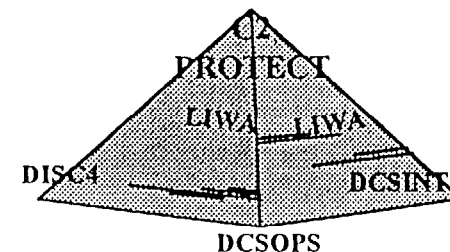C2 Protect - "Keeping The Highway Secure & Open For Force XXI"

Information Warfare Is:
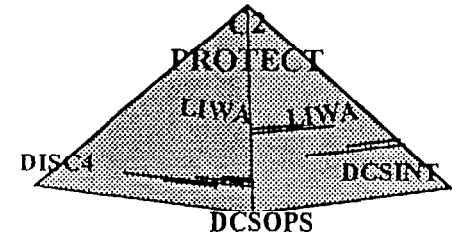
Is This New ?

- Old Security Disciplines Refocused
- An Integrated Strategy
- A Changing Paradigm
- An Operational Tool for the Commander
- A Combat Multiplier
- DODs Evolution into the Information Wave

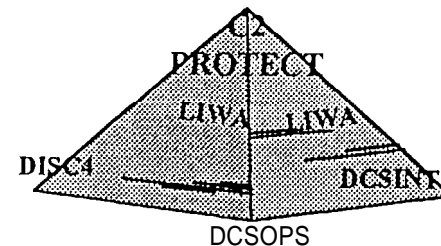C2 Protect - "Keeping The Highway Secure & Open For Force XXI"

Tasking

- Address information system security issues for the digital battlefield f ocus initial efforts on Task Force XXI AWE

- Address policy for planned demonstrations

- Conduct initial security review of documentation supporting Task Force XXI AWE

Threats and Vulnerabilities to **C2 Information Systems**

C2 INFORMATION SYSTEMS

MALICIOUS CODE

NATURAL DISASTERS

FOREIGN INTEL

POOR SSE

FUNDING

RF EFFECTS

POLICY

HACKERS

INSIDERS

VIRUSES

CRIMINAL ELEMENT

UNTRAINED USERS

UNTRAINED SYSTEM ADMINISTRATORS

TERRORISTS

INTERNET SURFING

PROTECT

LIWA   LIWA

DISC4   DCSINT

DCSOPS
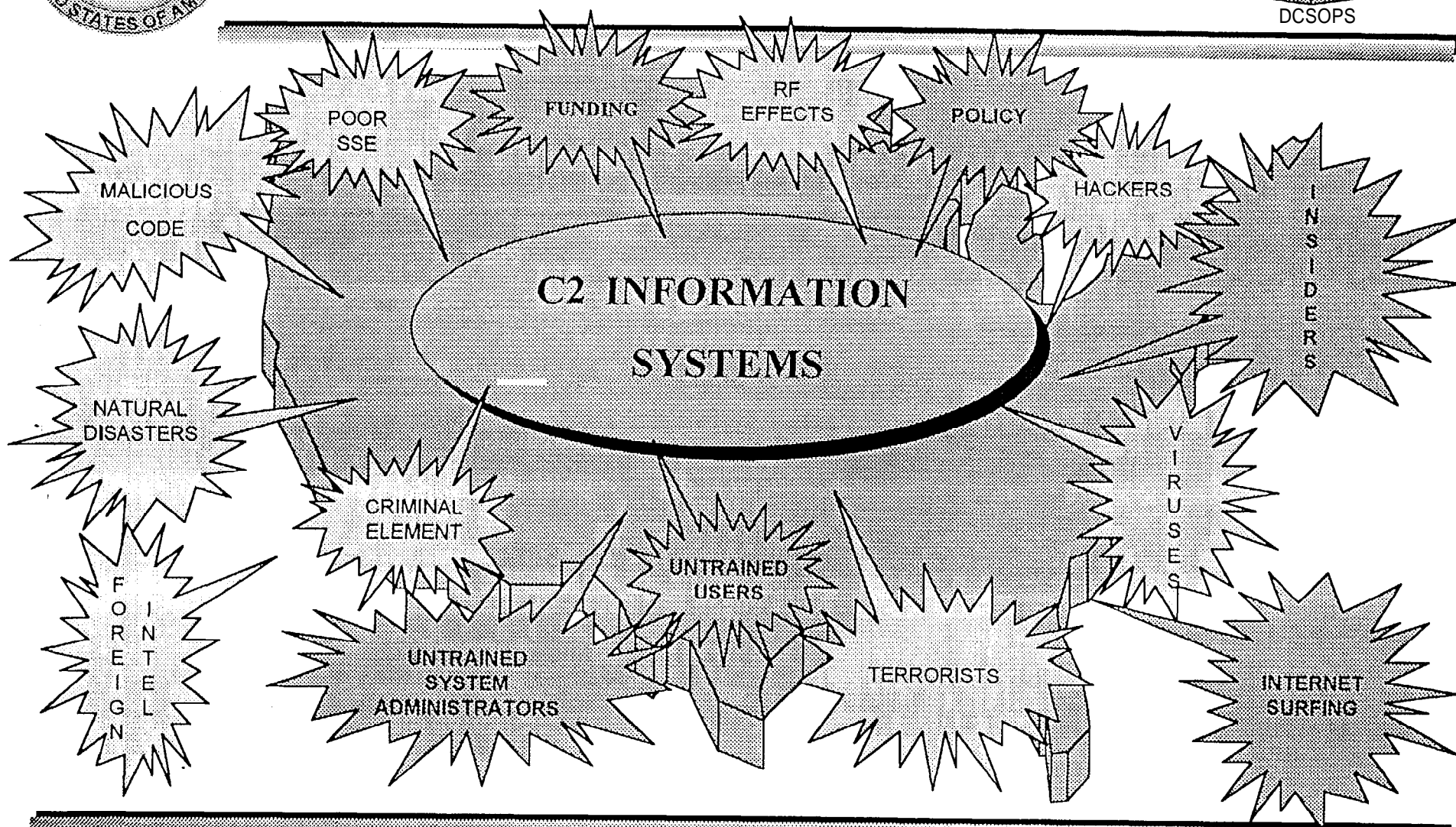
C2 Protect - "Keeping The Highway Secure & Open For Force XXI"

C2 Protect Development and Approach
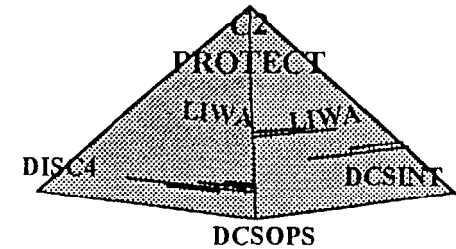
- Information Dominance is the New "High Ground" Current Intelligence is key.

- Protect, Detect, and React

- C2 Protect Program Management Plan: Multiple Activities with Multiple Security Disciplines

- Training, Personnel (Spaces and Faces), Tools

- Near Term Action Items from the C2 Protect & AISS Council of Colonels

- Long Term C2 Protect Resourcing

Legal, Policy and Regulatory
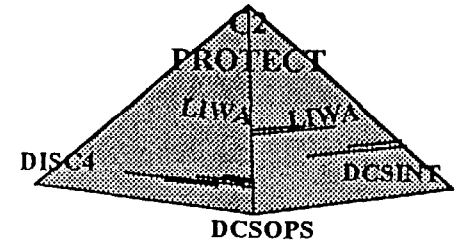
- **What is the sensitivity of information being processed?**
  What defined security levels are represented?
- **Where is the boundary for classified information as opposed to information we must protect?**
- **What is the structure for Accreditation?**
  Who is the Accreditor?
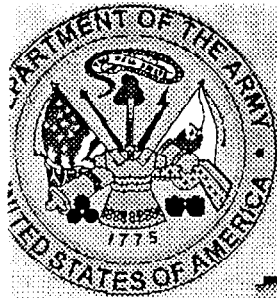
Purpose of Army C2 Protect Initiatives & Efforts
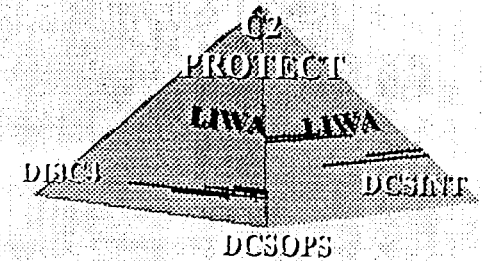
- Protect the Army's Portion of the Defense Information Infrastructure (DII)
- Synchronize Army Activities in C2 Protect
- Identify Vulnerabilities and Constraints
- Define Army Staff and MACOM Roles for C2 Protect
- Floor Plan for C2 Protect Developments
- Plan for C2 Protect Resources

C2 **Protect** Development Concerns
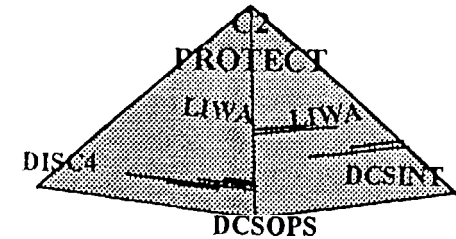
- Inadequate User and System Administration Training
- Funding and Resources
- Inadequate Protect and Detect Capability
- Army Computer Emergency Response Team (CERT)
- Validated Threat
- Information Sharing Infrastructure
- System Security Engineering Emphasis
- Sustaining Base Systems Focus

Training and Awareness is Key to C2 Protect
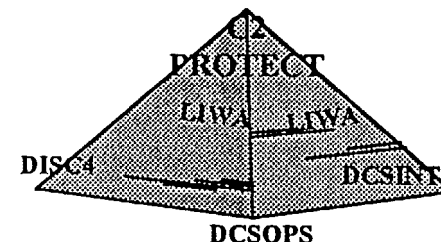
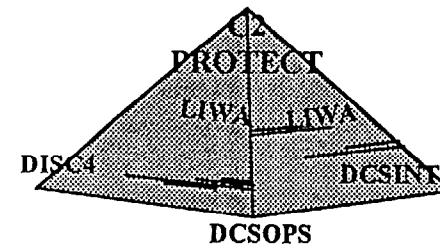"Our Troops must understand the threat and we must provide the leadership to minimize it".

"We must integrate Information Warfare realism into training the force"

LTG Guenther
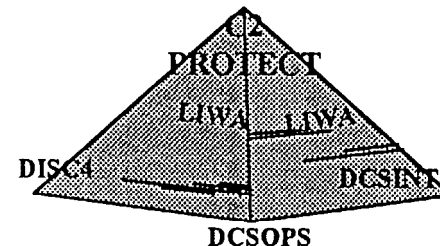HQDA, DISC4
29 Mar 95

C2 PROTECT
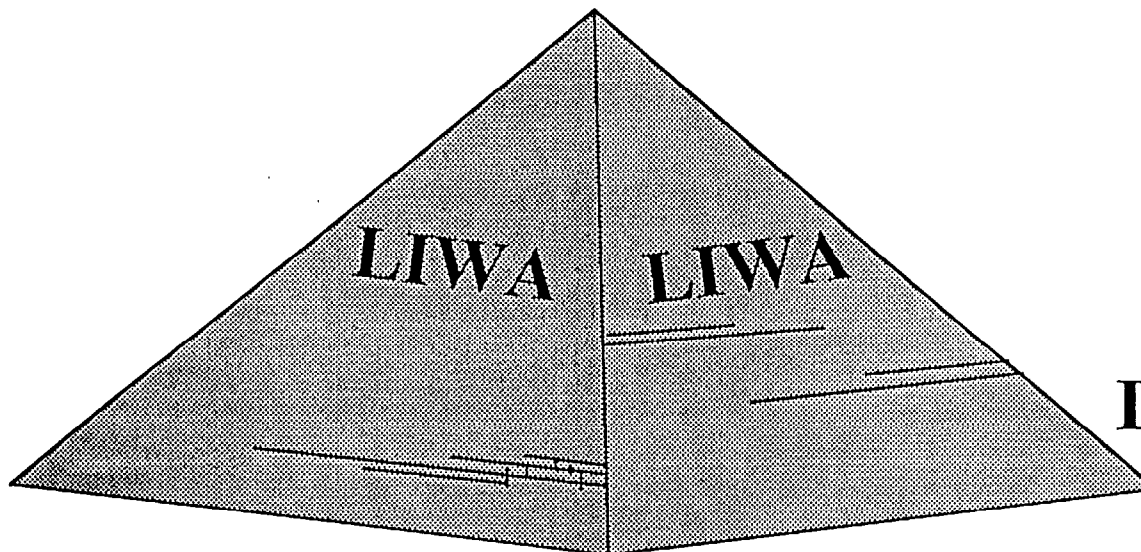
DISC4

DCSINT

DCSOPS

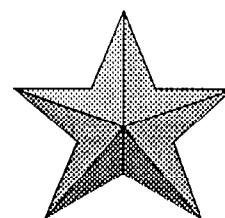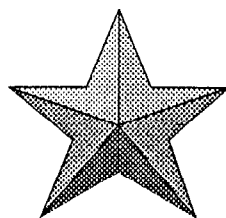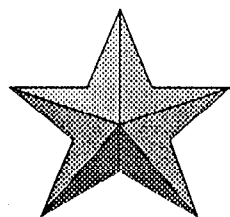Lead Developers and Signatures on all C2 Protect Volumes

C2 Protect - "Keeping The Highway Secure & Open For Force XXI"
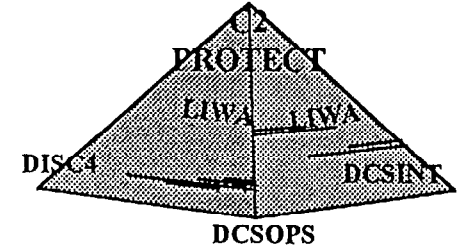
DISC4 C2 Protect Mission

In coordination with DCSOPS and DCSINT, DISC4 is responsible for implementing procedural and material protective measures, to protect Command, Control, Communications, and Computers (C4 Protect).
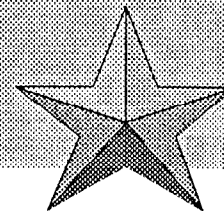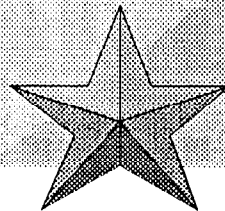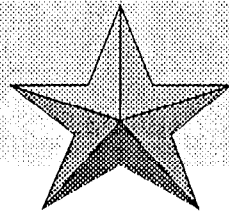
C2 Protect - "Keeping The Highway Secure & Open For Force XXI"
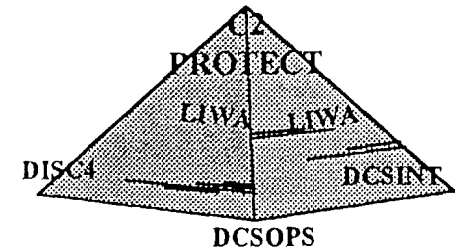
DCSINT C2 Protect Mission

In coordination with DCSOPS and DISC4, DCSINT is the office responsible for threat definition, establishment of policy and integrating counter-intelligence support to protect command control communications and computers (C4 Protect)
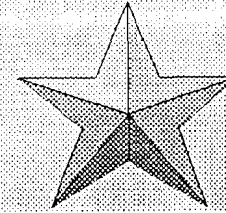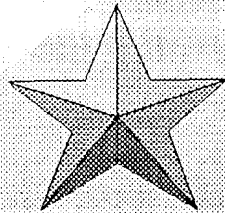
C2 Protect - "Keeping The Highway Secure & Open For Force XXI"
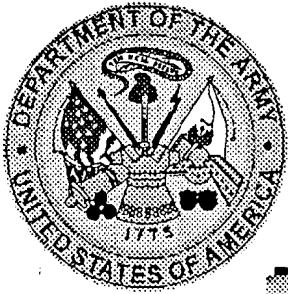
DCSOPS C2 Protect Mission

The DCSOPS is the organization which has proponancy for Information Warfare and addresses force modernization issues related to Information Warfare. Operational issues concerning Information Warfare are handled within the Directorate for Operations, Readiness, and Mobilization. DAMO-FDN is responsible for the development and dissemination of Information Warfare Policy for the Army.

Land Information Warfare Activity

DISC4   PROTECT   C2   LIWA   LIWA   DCSINT
DCSOPS

"LI WA"

MISSION:

Provide DA level Information Warfare/Command and Control Warfare support to Land Components and separate Army commands to facilitate planning and execution of Information Operations. Coordinate with National, Joint, and Service IW/C2W centers to exchange and synchronize intelligence and information support across the operational continuum.

C2 Protect - "Keeping The Highway Secure & Open For Force XXI"

Land Information Warfare Activity

✓ Act as Operational Focal Point for IW
Army Staff **(DCSOPS/DCSINT/DISC4)**
Joint, Service, and National Agencies
MACOMs and **MSCs**

✓ Arrange for and Coordinate Support to **CDRs**

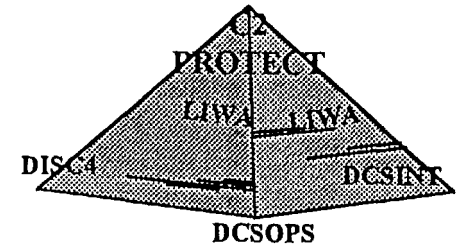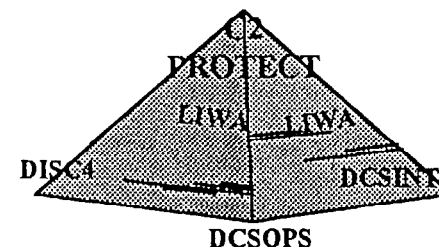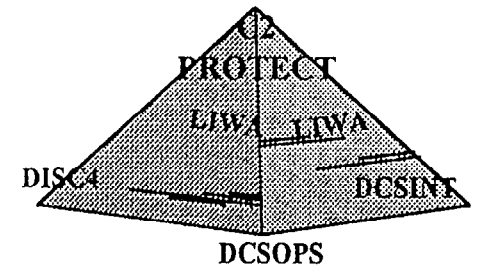✓ Coordinate and Deploy Field Support Teams

✓ Integrate Compartmented Programs with Other
Activities

C2 Protect - "Keeping The Highway Secure & Open For Force XXI"

DCSOPS

C2 Protect Issues

- **Computer Security**
  Software / Firmware Assurance Requirements
  Storage Media
  Output Media
  Certification
  Anti-Virus Protection
  Passwords

- **Security Services**
  Confidentiality
  Availability
  Integrity
  Identification and Authentication
  Access Control
  Non-repudiation

- **Communications Security**
  Key Distribution
  Key Management

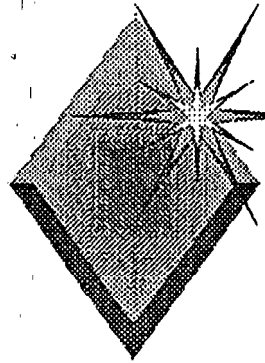- **Network Security**
  Routers (IP Routing Tables)
  Tactical Name Server
  IP to Host Domain Names
  Firewalls, Guards
  In-line Network Encryptors
  Limitations
  Security Management

- **Personnel Security**

- **Security Standards**

C2 Protect - "Keeping The Highway Secure & Open For Force XXI"

Army Information Sys terns are Under Attack

- ◆ Attacks are frequent and highly sophisticated
- ◆ Army had <u>90 reported penetrations</u> in CY 94
- ◆ **95%** of detected penetrations go unreported
- ◆ This means that Army had **1800** <u>detected</u>
- ◆ **94%** of penetrations are undetected
- ◆ Total penetrations to Army approx <u>4500</u>
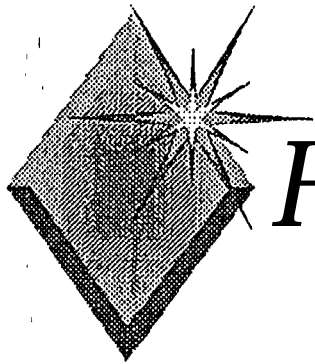
How Do Intruders Get In

- ◆ Through commercial service providers
  - ◆ 95% of of DOD comms use commercial service   ,
  - ◆ MILNET is mostly leased commercial service
- ◆ Run automated attack
  - ◆ Use software utility tools to obtain system info
 - ◆ Exploit system info to get user access
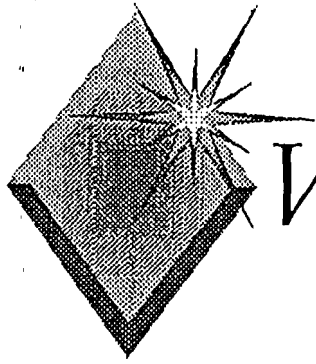
What Intruders Can Do

- ◆ Obtain password file
- ◆ Obtain system administrator privileges
- ◆ Plant undetectable programs
- ◆ Change, alter or destroy information
- ◆ Shut down system (now or later)
- ◆ Log on to next system as valid user
  - ◆ Down stream liability issue
  - ◆ Makes Army responsible for damage
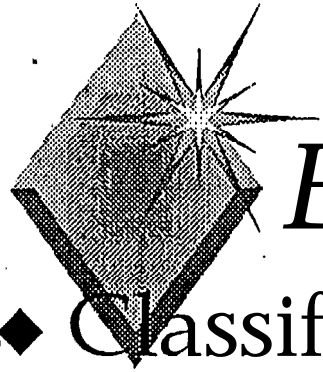
Example Internal Hacking

◆ Classified info on unclas MILNET

  ◆ OSD budget info

  ◆ DIA reports with names & locations of indivuals

  ◆ Air Force flights with dates, times, code names etc.

◆ Civ & Mil (AF) passing info to hacker network

◆ Member of Inaugration team selling access to BCN

◆ Users from HQ DA extracing pornographic material & games
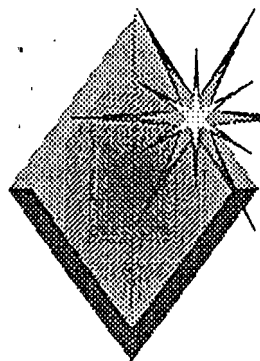
# *Example* of *Penetrations of Army Systems*

◆ ODISC4 LAN

- ◆ Requested Vulnerability analysis by SAM
- ◆ Used commonly available software tools
- ◆ Penetrated in 5 min
- ◆ Gained superuser (ROOT) access in 15 min
- ◆ Potential impact total enemy control plus
- ◆ trusted launching platform to other syst
- ◆ Penetration was not noticed or reported
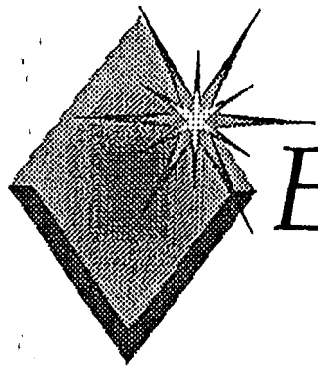
Example - JAG LAN

- Hackers from Denmark
- Stole information
- When hackers were discovered, system was shut down
- Minutes after bringing system up the hackers returned and took control
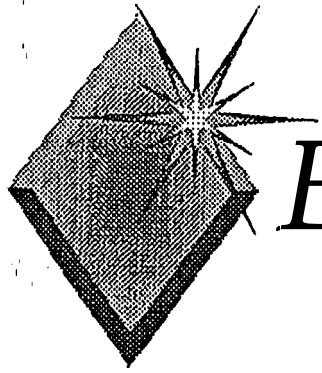
Example of Penetrations

◆ DSS-W

  ◆ 3 MB of data stolen

  ◆ data involved contract sensitive information

  ◆ ISC-P stopped the attack

 ◆ ISC-P assisted in p&venting subsequent attacks
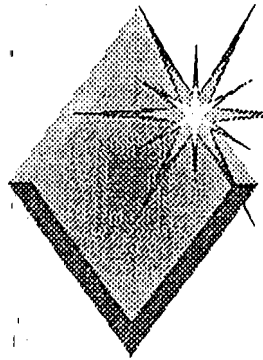
Example - Pentagon Broadband Cable Network (BCN)

- ◆ Unauthorized user from Swedish host logged in
  - ◆ Executed several commands
  - ◆ Posible loss of password file
- ◆ Unauthorized user from Virgina Tech host
  - ◆ Repeated attempts using various user IDs
  - ◆ Sucessful using system admimistrator's ID
- ◆ Unauthorized user from NASA host
  - ◆ Logged into two different user accounts

Infofmation Security
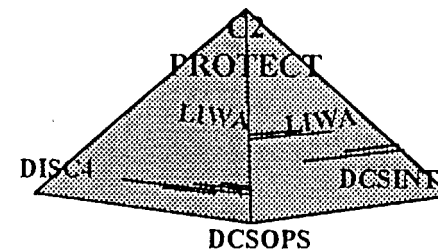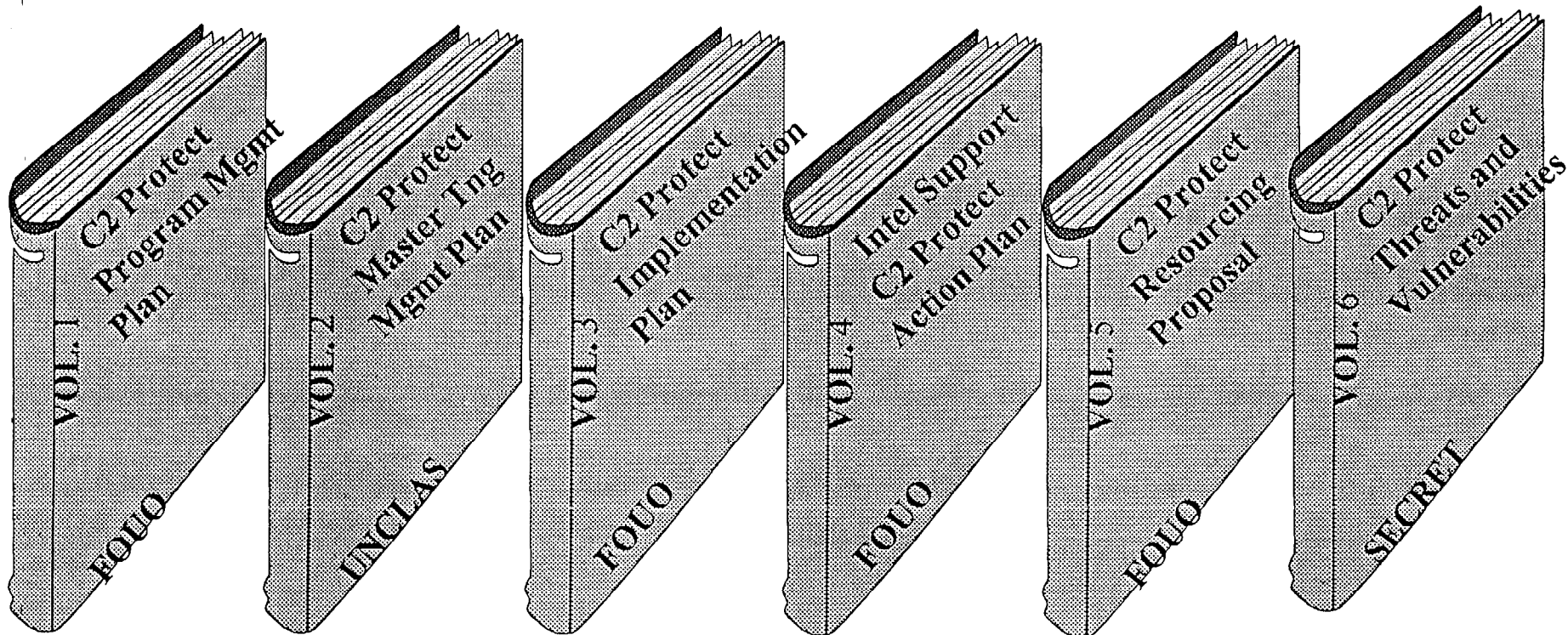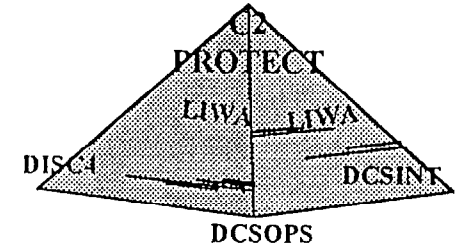
☑ **Education/Awareness**

☑ **Training**

☑ **Public Forums**
   Army Information Systems Security Council

☑ **Policies and Procedures**
   * The Army Plan
   * AR 38049
☑ * AR 25/70 series

☑ **Land Information Warfare Activity**

Army C2 Protect Library

- VOL. 1: C2 Protect Program Mgmt Plan — FOUO
- VOL. 2: C2 Protect Master Tng Mgmt Plan — UNCLAS
- VOL. 3: C2 Protect Implementation Plan — FOUO
- VOL. 4: Intel Support C2 Protect Action Plan — FOUO
- VOL. 5: C2 Protect Resourcing Proposal — FOUO
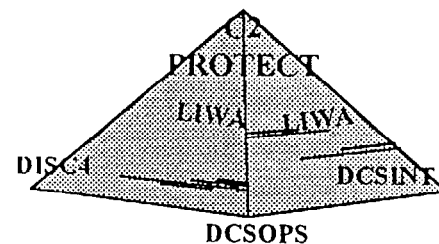- VOL. 6: C2 Protect Threats and Vulnerabilities — SECRET

C2 Protect Planning Evolves into AR XXX-XX

C2 Protect - "Keeping The Highway Secure & Open For Force XXI"

C2 Protect Working Group

Current Members

DISC4 (Chair Mr. Loranger)
   (Chair Mrs. Bailey)
IIAC   (Chair MAJ Ptaszynski)

DCSINT (Mr. Henson)
DCSOPS (Mr. McDowell)
NII (Mr. Denison)
USATRADOC(Mr. Giffin)
USASIGCEN(Mr. Riddle/Kidd)
USAICS (LTC Mitchell)
USAISC (Mr. Reardon)
USAMC (Mr. Poh)
LIWA (Mrs. Schalestock)

PEO IEW (Mr Rabb)
USAINSCOM (CPT Wade)
DCSPER (LTC Brown)
DCSLOG (DALO-ZB)
OCAR (
SARDA (Mr York)
DISA (D34 & CISS)
PEOC3 (TBD)
AGC (Mr Rothlein)
USACAC (Mr. Jackson)
NGB (Mr. Marsteller)
NSA (DR MaConachy)
ADO (Mr Balough)
USA CAC (TPIO)
USAFORCMD (Mr Horton)

C2 Protect - "Keeping The Highway Secure & Open For Force XXI"

ARMY.. ISSP REQUIREMENTS
WITHIN FUNDING PEGS
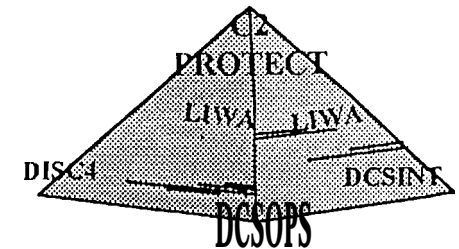
MODERNIZATION PEG

AIRTERM

BENIGN FILL

AKMS TIER 1 (EKMS)
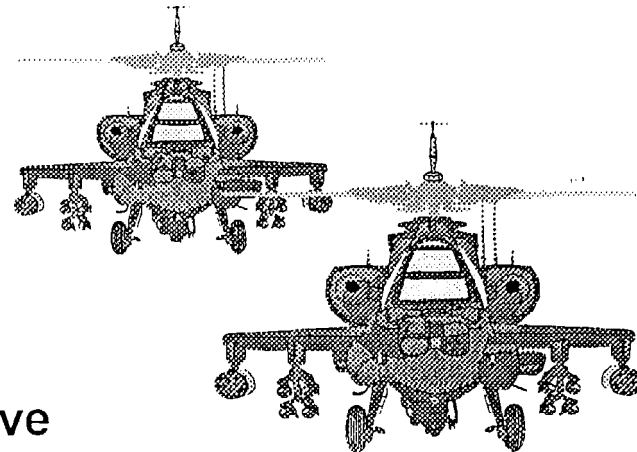
SECURE TERMINAL EQUIPMENT

KIV-7

KG-40A

Multi Information System Security Initiative
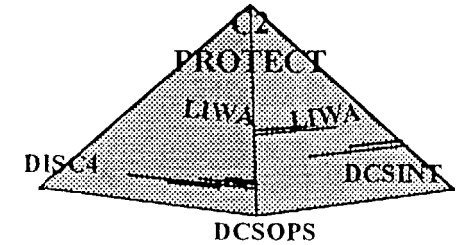
INFORMATION MANAGEMENT PEG
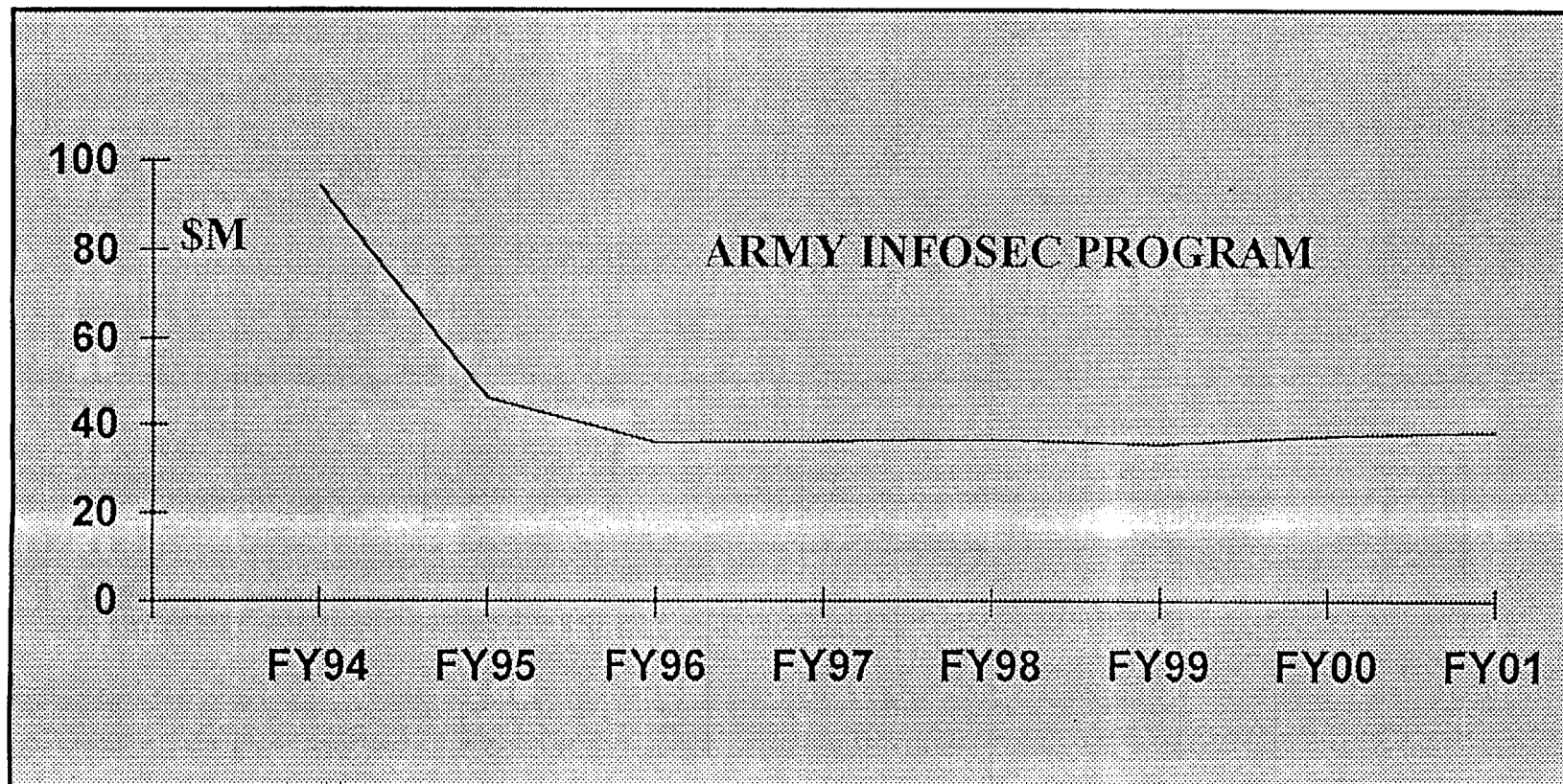
Defense Message System

MACOM

COMPUSEC

ARMY ISSP FY94-01

FY94	FY95	FY96	FY97	FY98	FY99	FY00	FY01
94.4 (52%)	45.9 (-22%)	35.7	36.0	36.5	35.4	37.3	38.3

ARMY INFOSEC PROGRAM

$M

100
80
60
40
20
0

FY94   FY95   FY96   FY97   FY98   FY99   FY00   FY01

C2 Protect - "Keeping The Highway Secure & Open For Force XXI"

Summary
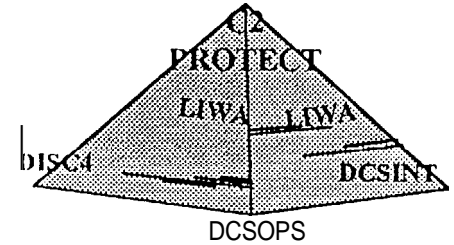
- Funding, Personnel, Resourcing and Intelligence Integration Remain Greatest Challenges

- Focus on Education, Training, and Awareness

- C2 Protect Roles and Responsibilities are Defined

- C2 Protect Master Training Management Plan and Program Management Plan are in Draft and C2 Protect Library identified and on Track

C2 Protect - "Keeping The Highway Secure & Open For Force XXI"